(A) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and

(B) Civil actions for damages and other appropriate remedies by the third party that reported the incident, as a third party beneficiary of the non-disclosure agreement.

(6) Use and release of contractor attributional/proprietary information created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this part that is created by or for DoD (including the information submitted pursuant to paragraph (b) of this section) is authorized to be used and released outside of DoD for purposes and activities authorized by this section, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(n) Contractors shall conduct their respective activities under this part in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(o) *Freedom of Information Act (FOIA).* Agency records, which may include qualifying information received from non-federal entities, are subject to request under the Freedom of Information Act (5 U.S.C. 552) (FOIA), which is implemented in the DoD by DoD Directive 5400.07 and DoD Regulation 5400.7–R (see 32 CFR parts 285 and 286, respectively). Pursuant to established procedures and applicable regulations, the Government will protect sensitive non-public information reported under mandatory reporting requirements against unauthorized public disclosure by asserting applicable FOIA exemptions. The Government will inform the non-Government source or submitter (*e.g.*, contractor or DIB participant of any such information that may be subject to release in response to a FOIA request), in order to permit the source or submitter to support the withholding of such information or pursue any other available legal remedies.

(p) *Other reporting requirements.* Cyber incident reporting required by this part in no way abrogates the contractor's responsibility for other cyber incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s), or as a result of other applicable U.S. Government statutory or regulatory requirements, including Federal or DoD requirements for Controlled Unclassified Information as established by Executive Order 13556, as well as regulations and guidance established pursuant thereto.

§ 236.5 DoD–DIB CS information sharing program.

(a) All contractors that are CDCs and meet the requirements set forth in § 236.7 are eligible to join the voluntary DoD–DIB CS information sharing program as a DIB participant.

(b) Under the voluntary activities of the DoD–DIB CS information sharing program, the Government and each DIB participant will execute a standardized agreement, referred to as a Framework Agreement (FA) to share, in a timely and secure manner, on a recurring basis, and to the greatest extent possible, cybersecurity information.

(c) Each such FA between the Government and a DIB participant must comply with and implement the requirements of this part, and will include additional terms and conditions as necessary to effectively implement the voluntary information sharing activities described in this part with individual DIB participants.

(d) The DoD–DIB CS Activities Office is the overall point of contact for the program. The DC3 managed DoD–DIB Collaborative Information Sharing Environment (DCISE) is the operational focal point for cyber threat information sharing and incident reporting under the DoD–DIB CS information sharing program.

(e) The Government will maintain a Web site or other internet-based capability to provide potential DIB participants with information about eligibility and participation in the program, to enable online application or registration for participation, and to

support the execution of necessary agreements with the Government.

(f) *GFI.* The Government shall share GFI with DIB participants or designated SP in accordance with this part.

(g) Prior to receiving GFI from the Government, each DIB participant shall provide the requisite points of contact information, to include security clearance and citizenship information, for the designated personnel within their company (*e.g.*, typically 3–10 company designated points of contact) in order to facilitate the DoD–DIB interaction in the DoD–DIB CS information sharing program. The Government will confirm the accuracy of the information provided as a condition of that point of contact being authorized to act on behalf of the DIB participant for this program.

(h) GFI will be issued via both unclassified and classified means. DIB participant handling and safeguarding of classified information shall be in compliance with DoD 5220.22–M, ''National Industrial Security Program Operating Manual (NISPOM),'' available at *http://www.dss.mil/documents/odaa/nispom2006-5220.pdf*. The Government shall specify transmission and distribution procedures for all GFI, and shall inform DIB participants of any revisions to previously specified transmission or procedures.

(i) Except as authorized in this part or in writing by the Government, DIB participants may:

(1) Use GFI only on U.S. based covered contractor information systems, or U.S. based networks or information systems used to provide operationally critical support; and

(2) Share GFI only within their company or organization, on a need-to-know basis, with distribution restricted to U.S. citizens.

(j) In individual cases DIB participants may request, and the Government may authorize, disclosure and use of GFI under applicable terms and conditions when the DIB participant can demonstrate that appropriate information handling and protection mechanisms are in place and has determined that it requires the ability:

(1) To share the GFI with a non-U.S. citizen; or

(2) To use the GFI on a non-U.S. based covered contractor information system; or

(3) To use the GFI on a non-U.S. based network or information system in order to better protect a contractor's ability to provide operationally critical support.

(k) DIB participants shall maintain the capability to electronically disseminate GFI within the Company in an encrypted fashion (*e.g.*, using Secure/Multipurpose Internet Mail Extensions (S/MIME), secure socket layer (SSL), Transport Layer Security (TLS) protocol version 1.2, DoD-approved medium assurance certificates).

(l) DIB participants shall not share GFI outside of their company or organization, regardless of personnel clearance level, except as authorized in this part or otherwise authorized in writing by the Government.

(m) If the DIB participant utilizes a SP for information system security services, the DIB participant may share GFI with that SP under the following conditions and as authorized in writing by the Government:

(1) The DIB participant must identify the SP to the Government and request permission to share or disclose any GFI with that SP (which may include a request that the Government share information directly with the SP on behalf of the DIB participant) solely for the authorized purposes of this program.

(2) The SP must provide the Government with sufficient information to enable the Government to determine whether the SP is eligible to receive such information, and possesses the capability to provide appropriate protections for the GFI.

(3) Upon approval by the Government, the SP must enter into a legally binding agreement with the DIB participant (and also an appropriate agreement with the Government in any case in which the SP will receive or share information directly with the Government on behalf of the DIB participant) under which the SP is subject to all applicable requirements of this part and of any supplemental terms and conditions in the DIB participant's FA with the Government, and which authorizes the SP to use the GFI only as authorized by the Government.

(n) The DIB participant may not sell, lease, license, or otherwise incorporate the GFI into its products or services, except that this does not prohibit a DIB participant from being appropriately designated an SP in accordance with paragraph (m) of this section.

§ 236.6 General provisions of the DoD–DIB CS information sharing program.

(a) Confidentiality of information that is exchanged under the DoD–DIB CS information sharing program will be protected to the maximum extent authorized by law, regulation, and policy. DoD and DIB participants each bear responsibility for their own actions under the voluntary DoD–DIB CS information sharing program.

(b) All DIB CS participants may participate in the Department of Homeland Security's Enhanced Cybersecurity Services (ECS) program (*http://www.dhs.gov/enhanced-cybersecurity-services*).

(c) Participation in the voluntary DoD–DIB CS information sharing program does not obligate the DIB participant to utilize the GFI in, or otherwise to implement any changes to, its information systems. Any action taken by the DIB participant based on the GFI or other participation in this program is taken on the DIB participant's own volition and at its own risk and expense.

(d) A DIB participant's participation in the voluntary DoD–DIB CS information sharing program is not intended to create any unfair competitive advantage or disadvantage in DoD source selections or competitions, or to provide any other form of unfair preferential treatment, and shall not in any way be represented or interpreted as a Government endorsement or approval of the DIB participant, its information systems, or its products or services.

(e) The DIB participant and the Government may each unilaterally limit or discontinue participation in the voluntary DoD–DIB CS information sharing program at any time. Termination shall not relieve the DIB participant or the Government from obligations to continue to protect against the unauthorized use or disclosure of GFI, attribution information, contractor proprietary information, third-party proprietary information, or any other information exchanged under this program, as required by law, regulation, contract, or the FA.

(f) Upon termination of the FA, and/or change of Facility Security Clearance (FCL) status below Secret, GFI must be returned to the Government or destroyed pursuant to direction of, and at the discretion of, the Government.

(g) Participation in these activities does not abrogate the Government's, or the DIB participants' rights or obligations regarding the handling, safeguarding, sharing, or reporting of information, or regarding any physical, personnel, or other security requirements, as required by law, regulation, policy, or a valid legal contractual obligation. However, participation in the voluntary activities of the DoD–DIB CS information sharing program does not eliminate the requirement for DIB participants to report cyber incidents in accordance with § 236.4.

§ 236.7 DoD–DIB CS information sharing program requirements.

(a) To participate in the DoD–DIB CS information sharing program, a contractor must be a CDC and shall:

(1) Have an existing active FCL granted under the NISPOM (DoD 5220.22–M); and

(2) Execute the standardized FA with the Government (available during the application process), which implements the requirements set forth in §§ 236.5 through 236.7, and allows the CDC to select their level of participation in the voluntary DoD–DIB CS information sharing program.

(3) In order for participating CDCs to receive classified cyber threat information electronically, they must:

(i) Have or acquire a Communication Security (COMSEC) account in accordance with the NISPOM Chapter 9, Section 4 (DoD 5220.22–M), which provides procedures and requirements for COMSEC activities; and

(ii) Have or acquire approved safeguarding for at least Secret information, and continue to qualify under the NISPOM for retention of its FCL and approved safeguarding; and